REMARKS.

Careful consideration has been given to the Official Action of January 19, 2007 and it is respectively submitted that the amendatory action which has been taken places the application into condition for allowance.

Claim Objections.

The Examiner has objected Claims 5-6 under 37 CFR 1.75(c). To meet the objection these two claims were rewritten as one new claim 5. Word "system" in this claim may refer, for example, to the system containing ATM, as it is illustrated in the end of Detailed Description of the Invention.

Claim Rejections.

The Examiner has rejected Claims 1-6 as being anticipated by Buffam (US-6185316-B1).

I respectfully disagree with the Examiner. The main difference between my application and Buffam's invention is as follows.

Buffam's invention.	My application.
"... conceals an encryption key within a structure such that the structure itself, or a representation thereof, is needed to recover the key". (First phrase of Detailed Description.)	There is no key at all. There is no encoding or hashing - just changing of the sequence of terms in the biometric array ("shuffling"). There is no decoding - just calculation of correlation coefficient.

This difference is important in achieving the main goal of the invention - privacy of user.

Indeed, "The existence of one-way functions is an open conjecture" (http://en.wikipedia.org/wiki/One-way_function) - their existence has not been proven and is an unsolved problem in computer science. In fact, another instrument, to which Buffam reffers as to the most secure algorithm and which had been commonly used and

relied on in cryptography - MD5 hash function - has already been found to have weekness. "In August 2004, researchers found weaknesses in a number of hash functions, including MD5" (http://en.wikipedia.org/wiki/Cryptographic_hash_function). Thus, at least theoretically, it is not impossible that an attacker can create a new mathematical method, invert one-way function, and restore both the key and the true biometrics. In this scenario the user looses the biometrical information forever.

On the other hand, if the order of sequence in biometric array is changed on the client by the user (which is proposed in my method), there is no theoretical possibility to restore initial order. Attacker has nothing to decode. He can change the order of terms in the stolen twisted signature, but he does not have criteria when to stop in order to restore the real signature: he has nothing to compare with. So, the privacy of the user in my method is assured in greater degree.

I believe this difference presents patentable novelty which the claims present in view of the references cited (Buffam, US-6185316-B1) and the rejection made ("anticipation").

Inventor  V.Gorelik.

2/8/2007